

Steven R. Dunbar  
Department of Mathematics  
203 Avery Hall  
University of Nebraska-Lincoln  
Lincoln, NE 68588-0130  
<http://www.math.unl.edu>  
Voice: 402-472-3731  
Fax: 402-472-8466

## Topics in Probability Theory and Stochastic Processes Steven R. Dunbar

---

### Card Shuffling as a Markov Chain

---

Note: These pages are prepared with MathJax. MathJax is an open source JavaScript display engine for mathematics that works in all browsers. See <http://mathjax.org> for details on supported browsers, accessibility, copy-and-paste, and other features.

---

[Rating]../../../CommonInformation/Lessons/rating.png

### Rating

Mathematically Mature: may contain mathematics beyond calculus with proofs.

---

[Section Starter Question]../../../CommonInformation/Lessons/question<sub>mark</sub>.png

## Section Starter Question

Why shuffle a deck of cards? What kind of shuffle do you use? How many shuffles are sufficient to achieve the purpose of shuffling?

---

[Key Concepts]../../../CommonInformation/Lessons/keyconcepts.png

## Key Concepts

1. Card deck shuffles are a family of possible re-orderings with probability distributions, leading to transition probabilities, and thus Markov processes. The most well-studied type of shuffle is the riffle shuffle and that is the main focus here.
2. Going from card order  $\pi$  to  $\tau$  is the same as composing  $\pi$  with the permutation  $\pi^{-1} \circ \tau$ . Now identify shuffles as functions on  $\{1, \dots, n\}$  to  $\{1, \dots, n\}$ , that is, permutations. Since a particular shuffle is one of a whole family of shuffles, chosen with a probability distribution  $Q$  from the family, the transition probabilities are

$$p_{\pi\tau} = \mathbb{P}[X_t = \tau \mid X_{t-1} = \pi] = Q(\pi^{-1} \circ \tau).$$

3. The identification of shuffles or operations with permutations gives a probability distribution on  $S_n$ .
4. A **Top-to-Random Shuffle**, takes the top card from a stack of  $n$  cards and inserts it in the gap between the  $(k-1)$ th card and the  $k$ th card in the deck.
5. The Top-To-Random-Shuffle demonstrates the cut-off phenomenon for the Total Variation distance of the Markov chain distribution from the uniform distribution as a function of the number of steps.
6. One realistic model of shuffling a deck of cards is the **riffle shuffle**.
7. The set of cuts and interleavings in a riffle shuffle induces in a natural way a density on the set of permutations. Call this a **riffle shuffle** and denote it by  $R$ . That is,  $R(\pi)$  is the sum of probabilities of each cut and interleaving that gives the rearrangement of the deck corresponding to  $\pi$ .

8. 7 shuffles the of 3-card deck gets very close to the uniform density, which turns out to be the stationary density.
9. The probability of achieving a permutation  $\pi$  when doing an  $a$ -shuffle is

$$\frac{1}{a^n} \binom{n+a-r}{n},$$

where  $r$  is the number of rising sequences in  $\pi$ .

10. The eigenvalues of the transition probability matrix for a riffle shuffle are  $1, \frac{1}{2}, \frac{1}{4}$  and  $\frac{1}{2^n}$ . The second largest eigenvalue determines the rate of convergence to the stationary distribution. For riffle shuffling, this eigenvalue is  $\frac{1}{2}$ .
11. For a finite, irreducible, aperiodic Markov chain  $Y_t$  distributed as  $Q^t$  at time  $t$  and with stationary distribution  $\pi$ , and  $\tau$  is a strong stationary time, then

$$\|Q^\tau - \pi\|_{TV} \leq \mathbb{P}[(\tau \geq t).$$

12. Set  $d_n(t) = \|P^{\tau_{\text{top}}+1} - U\|_{TV}$ . Then for  $\epsilon > 0$ ,
  - (a)  $d_n(n \log n + n \log \epsilon^{-1}) \leq \epsilon$  for  $n$  sufficiently large.
  - (b)  $d_n(n \log n - n \log(C\epsilon^{-1})) \geq 1 - \epsilon$  for  $n$  sufficiently large.

---

[Vocabulary]../../../CommonInformation/Lessons/vocabulary.png

## Vocabulary

1. A **Top-to-Random Shuffle**, takes the top card from a stack of  $n$  cards and inserts it in the gap between the  $(k-1)$ th card and the  $k$ th card in the deck.
2. The **total variation distance** of  $\mu$  from  $\nu$  is

$$\|\mu - \nu\|_{TV} = \max_{A \subset \Omega} |\mu(A) - \nu(A)| = \frac{1}{2} \sum_{x \in \Omega} |\mu(x) - \nu(x)|.$$

3. A **strong stationary time** for  $X_t$ ,  $t \geq 0$  if  $X_{\tau_{\text{top}}+1} \sim \text{unif}(S_n)$ , and  $X_{\tau_{\text{top}}+1}$  is independent of  $\tau_{\text{top}}$ .
4. The **riffle shuffle** first cuts the deck randomly into two packets, one containing  $k$  cards and the other containing  $n - k$  cards. Choose  $k$ , the number of cards cut according to the binomial density. Once the deck is cut into two packets, interleave the cards from each packet in any possible way, such that the cards from each packet keep their own relative order.
5. A special case of this is the **perfect shuffle**, also known as the **faro shuffle** wherein the two packets are completely interleaved.
6. A **rising sequence** of a permutation is a maximal consecutive increasing subsequence.
7. A  **$a$ -shuffle** is another probability density on  $S_n$ . Let  $a$  be any positive integer. Cut the deck into  $a$  packets of nonnegative sizes  $m_1, m_2, \dots, m_a$  with  $m_1 + \dots + m_a = n$  but some of the  $n_i$  may be zero. Interleave the cards from each packet in any way, so long as the cards from each packet, so long as the cards from each packet keep the relative order among themselves. With a fixed packet structure, consider all interleavings equally likely.

---

[Mathematical Ideas]../../../CommonInformation/Lessons/mathematicalideas.png

## Mathematical Ideas

### General Setting

An unopened deck of cards has the face-up order (depending on manufacturer, but typically in the U.S.), starting with the Ace of Spades:

- Ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, Jack, Queen, King of Spades,
- Ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, Jack, Queen, King of Diamonds,
- King, Queen, Jack, 10, 9, 8, 7, 6, 5, 4, 3, 2, Ace of Clubs, then

- King, Queen, Jack, 10, 9, 8, 7, 6, 5, 4, 3, 2, Ace of Hearts.

Call this the initial order of the deck. Knowing this order is essential for some sleight of hand tricks performed by a magician. For card players, shuffling the deck to remove this order is essential so that cards dealt from the deck come “at random”, that is, in an order uniformly distributed over all possible deck orders. The main question here is: Starting from this order, how many shuffles are necessary to obtain a “random” deck order from the uniform distribution?

In terms of Markov processes, the questions are: What is the state space, what is an appropriate transition probability matrix, what is the steady state distribution, hopefully uniform, and how fast does the Markov process approach the steady state distribution?

For simplicity and definiteness, let the cards in the initial deck order above be numbered 1 to 52. It will also be convenient to study much smaller decks of cards having  $n$  cards. The set of states for a Markov process modeling the order of the deck is  $S_n$ , the set of permutations on  $n$  cards. For convenience, set the initial state  $X_0$  to be the identity permutation with probability 1. In other words, choose the initial distribution as not shuffling the deck yet.

Consider a shuffle, that is, a re-ordering operation on a state that takes an order to another order. For example, the riffle shuffle, also called a dovetail shuffle or leafing the cards, is a common type of shuffle that interleaves packets of cards. A perfect riffle shuffle, also called a faro shuffle, splits the deck exactly in half, then interleaves cards alternately from each half. A perfect riffle shuffle is difficult to perform, except for practiced magicians. More commonly, packets of adjacent cards from unevenly split portions interleave, creating a new order for the deck that nevertheless preserves some of the previous order in each packet. Thus a particular riffle shuffle is one of a whole family of riffle shuffles, chosen with a probability distribution on the family. This probability distribution then induces a transition probability from state to state, and thus a Markov process.

Other types of shuffles have colorful names such as the Top-to-Random shuffle, Hindu shuffle, pile shuffle, Corgi shuffle, Mongean shuffle, and Weave shuffle. Some shuffle types are a family of possible re-orderings with probability distributions different from the riffle shuffle, leading to different transition probabilities, and thus different Markov processes.

Going from card order  $\pi$  to  $\sigma$  is the same as composing  $\pi$  with the permutation  $\pi^{-1} \circ \sigma$ . Now identify shuffles as functions on  $\{1, \dots, n\}$  to  $\{1, \dots, n\}$ ,

that is, permutations. Since a particular riffle shuffle is one of a whole family of riffle shuffles, chosen with a probability distribution  $Q$  from the family, the transition probabilities are  $p_{\pi\sigma} = \mathbb{P}[X_t = \sigma \mid X_{t-1} = \pi] = Q(\pi^{-1} \circ \sigma)$ . So now the goal is to describe the probability distribution  $Q$  and apply it to the Markov process.

*Remark.* This section uses a list notation for permutations. For example, the notation  $\pi = [231]$  represents the permutation with  $\pi(1) = 2$ ,  $\pi(2) = 3$  and  $\pi(3) = 1$ . A common alternative explicit notation for the same permutation is

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Writing the permutation in matrix form makes finding the inverse obvious,  $\pi^{-1} = [312]$ .

Recall also that sequential permutations are applied from right to left. Composing  $\pi$  with the permutation  $\pi^{-1} \circ \sigma$  gives  $\pi \circ (\pi^{-1} \circ \sigma) = \sigma$ . If  $\sigma = [132]$ , then  $\pi^{-1} \circ \sigma = [321]$  and  $[132] = [231] \circ [321]$ .

This section does not use cycle notation for permutations.

## Top to Random Shuffle

A particularly simple shuffle is the **Top-to-Random Shuffle**, abbreviated TTRS. The TTRS takes the top card from a stack of  $n$  cards and inserts it in the gap between the  $(k-1)$ th card and the  $k$ th card in the deck. See Figure 1. Note that  $k=1$  is possible, in which case the top card returns to the top. Likewise,  $k=n+1$  is also permitted, in which case the top card moves to the bottom of the card stack.

Consider the order of the cards to be a permutation on  $n$  symbols. The TTRS is naturally a finite Markov chain  $X_t$  for  $t \geq 0$  with  $X_t \in S_n$ . Set  $X_0 = \sigma_0$ , the identity permutation. The transition probabilities are

$$\mathbb{P}[X_{t+1} = \sigma' \mid X_t = \sigma] = \begin{cases} \frac{1}{n} & \sigma' \text{ is a TTRS of } \sigma \\ 0 & \text{otherwise} \end{cases}$$

defining the transition probability matrix  $P$ . Then after  $t$  TTRS shuffles, the order of the deck has a probability distribution  $P^t X_0$  on  $S_n$ , where with an overload of notation  $X_0$  is the vector with a 1 in the position for  $\sigma_0$  and 0 elsewhere, representing the initial state. The Markov chain  $X_t$  induced by the TTRS is irreducible, see the exercises. It is also immediate that  $X_t$

is aperiodic since it is possible that the top card can recur back on top. Therefore, this Markov chain must converge to a stationary distribution and this section will later prove that  $P^t X_0 \rightarrow \text{unif}(S_n)$ .

*Example.* The transition matrix for the TTRS on a deck with three cards is

$$\begin{matrix} & [123] & [213] & [231] & [132] & [312] & [321] \\ \begin{matrix} [123] \\ [213] \\ [231] \\ [132] \\ [312] \\ [321] \end{matrix} & \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & 0 & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & \frac{1}{3} \end{pmatrix} \end{matrix}.$$

If the card deck is initially in order 1 to  $n$  from top to bottom, how many TTRS shuffles does it take for the deck to be sufficiently shuffled? Starting with the identity ordering, the density of the permutations after 7 top-to-random shuffles is the first row of  $P^7$ . Numerically,

$$P^7 = \begin{pmatrix} 0.16690 & 0.16690 & 0.16690 & 0.16644 & 0.16644 & 0.16644 \\ 0.16690 & 0.16690 & 0.16644 & 0.16690 & 0.16644 & 0.16644 \\ 0.16644 & 0.16644 & 0.16690 & 0.16644 & 0.16690 & 0.16690 \\ 0.16644 & 0.16644 & 0.16644 & 0.16690 & 0.16690 & 0.16690 \\ 0.16690 & 0.16644 & 0.16644 & 0.16690 & 0.16690 & 0.16644 \\ 0.16644 & 0.16690 & 0.16690 & 0.16644 & 0.16644 & 0.16690 \end{pmatrix}.$$

That is, 7 shuffles of the 3-card deck gets close to the stationary density, which turns out to be the uniform density. The eigenvalues of  $P$  are  $1, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, 0, 0$ .

**Lemma 1.** *At any time  $t$ , if  $k$  cards appear beneath the card labeled  $n$ , then these cards appear in any order with equal probability.*

*Proof.* The proof is by induction on  $t$ . The base case  $t = 0$  is trivial. Suppose that the claim is true for some  $t > 0$ . In the transition to  $t + 1$ , two cases can occur, see Figure 2 for a schematic diagram. First, the top card is randomly placed above the card labeled  $n$  that is somewhere in the stack. Then nothing is changed and the proof is complete. Otherwise, the top card is placed in one of the  $k + 1$  available spaces below the last card labeled  $n$  that is somewhere in the stack. The probability of any particular one of these arrangements is

$$\frac{1}{k!} \cdot \frac{1}{k+1} = \frac{1}{(k+1)!}$$

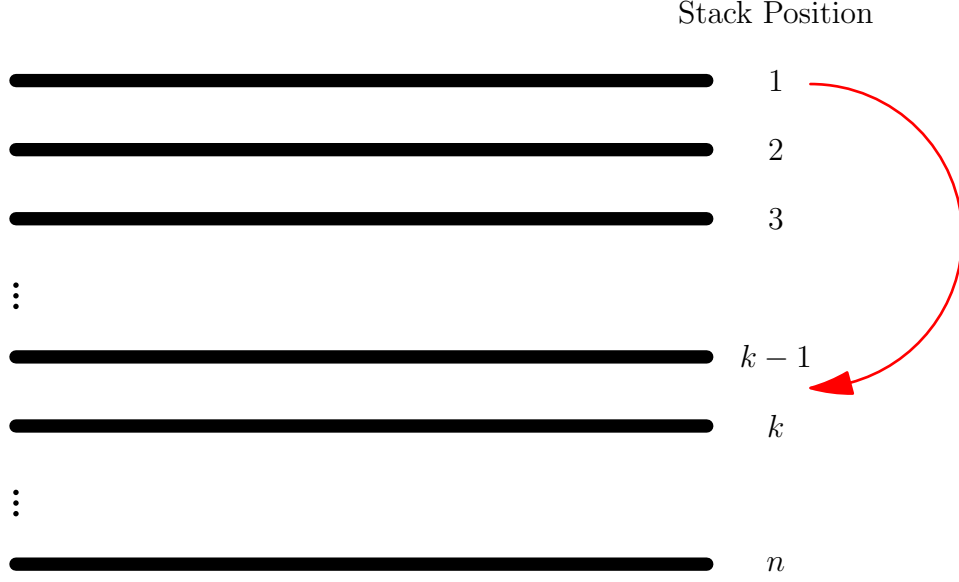


Figure 1: Schematic drawing of the Top-to-Random-Shuffle.



Figure 2: Schematic diagram of the proof of the Lemma.

where  $\frac{1}{k!}$  comes from the induction hypothesis and the  $\frac{1}{k+1}$  comes from the TTRS. The proof is complete.  $\square$

**Theorem 2.** *Let  $\tau_{top}$  be the first time that card  $n$  reaches the top of the deck. Then  $P^{\tau_{top}+1}X_0$  is uniform on  $S_n$ . Furthermore, whatever permutation arises at time  $\tau_{top} + 1$  is independent of  $\tau_{top}$ .*

*Proof.* The proof follows from the Lemma, since at time  $\tau_{top}$  the  $n - 1$  cards below card  $n$  will be uniformly distributed over the  $(n - 1)!$  possible permutations. Then at time  $\tau_{top} + 1$  card  $n$  is inserted uniformly at random in the deck.  $\square$

*Remark.* Waiting for  $\tau_{top}$  is the same as waiting for completion in the “coupon collectors problem in reverse”. More precisely, collecting a coupon here is



putting the top card below the card labeled  $n$ . The first card is hard to put under  $n$ , in fact it happens with probability  $\frac{1}{n+1}$  but it gets easier as time goes on. This motivates the later assertions that  $\mathbb{E}[\tau_{\text{top}} + 1] = \Theta(n \log n)$  and that  $\mathbb{P}[\tau_{\text{top}} + 1 \geq n \log n + cn] \leq e^{-c}$  for all  $c \geq 0$ . See below for more details.

*Definition.* If  $\mu$  and  $\nu$  are probability distributions on  $\Omega$ , the **total variation distance** of  $\mu$  from  $\nu$  is

$$\|\mu - \nu\|_{TV} = \sup_{A \subset \Omega} |\mu(A) - \nu(A)| = \frac{1}{2} \sum_{x \in \Omega} |\mu(x) - \nu(x)|.$$

*Remark.* Probability distributions  $\mu$  and  $\nu$  are far apart in total variation distance if there is a “bad event”  $A$  such that  $\mu$  and  $\nu$  measure  $A$  differently.

*Definition.* Define  $\tau_{\text{top}}$  as a **strong stationary time** for  $X_t$ ,  $t \geq 0$  if  $X_{\tau_{\text{top}}+1} \sim \text{unif}(S_n)$ , and  $X_{\tau_{\text{top}}+1}$  is independent of  $\tau_{\text{top}}$ .

*Remark.* A *stopping time* is a rule which tells the process to “stop” depending on the current value of the process. The stopping time is strong stationary if conditional on stopping after  $t + 1$  steps the value of the process is uniform on the state space.

**Lemma 3.** *Let  $Q$  be a probability distribution on a finite group  $G$  inducing an irreducible and aperiodic Markov chain with transition probabilities  $Q(\pi^{-1} \circ \sigma)$  from  $\pi$  to  $\sigma$ . Let  $\tau$  be a strong stationary time for  $Q$  and  $U$  the uniform distribution. Then*

$$\|Q^\tau - U\|_{TV} \leq \mathbb{P}[\tau > k]$$

for all  $k \geq 0$

*Remark.* The hypotheses irreducible and aperiodic may not be strictly necessary, but occur here because both are common in theorems about Markov chains.

*Proof.* For any  $A \subset G$

$$\begin{aligned} Q^k(A) &= \mathbb{P}[X_k \in A] \\ &= \sum_{j \leq k} \mathbb{P}[X_k \in A, \tau = j] + \mathbb{P}[X_k \in A, \tau > k] \\ &= \sum_{j \leq k} U(A) \mathbb{P}[\tau = j] + \mathbb{P}[X_k \in A \mid \tau > k] \mathbb{P}[\tau > k] \\ &= U(A) + (\mathbb{P}[X_k \in A \mid \tau > k] - U(A)) \mathbb{P}[\tau > k] \end{aligned}$$

and because  $|\mathbb{P}[X_k \in A \mid \tau > k] - U(A)| \leq 1$

$$\|Q^\tau - U\|_{TV} \leq \mathbb{P}[\tau > k].$$

□

**Lemma 4.** *Sample uniformly with replacement from an urn with  $n$  balls. Let  $V$  be the number of draws required until each ball has been drawn at least once. Then*

$$\mathbb{P}[V > n \log n + cn] \leq e^{-c}$$

for  $c \geq 0$  and  $n \geq 1$ .

*Remark.* The lemma statement is another formulation of the coupon collectors problem. The usual formulation has  $n$  different types of coupons or prizes in a cereal box. On each draw, one obtains a coupon or prize equally likely to be any one of the  $n$  types. The goal is to find the expected number of coupons one needs to gather before obtaining a complete set of at least one of each type.

*Proof.* Let  $m = n \log n + cn$ . For each ball  $b$  let  $A_b$  be the event “ball  $b$  not drawn in the first  $m$  draws. Then

$$\mathbb{P}[V > m] = \mathbb{P}\left[\bigcup_{b=1}^n A_b\right] \leq \sum_{b=1}^n \mathbb{P}[A_b] = n \left(1 - \frac{1}{n}\right)^m \leq ne^{-m/n} = e^{-c}.$$

See the exercises for a proof of the second inequality. □

For simplicity in what follows, set  $d_P(n) = \|P^n - U\|_{TV}$ . Then  $d_P(n)$  measures how close  $n$  repeated shuffles get the deck to being shuffled according to the uniform density.

**Theorem 5.** *For the TTRS shuffle*

1.  $d_P(n \log n + n \log \epsilon^{-1}) \leq \epsilon$  for  $n$  sufficiently large.
2.  $d_P(n \log n - n \log(C\epsilon^{-1})) \geq 1 - \epsilon$  for  $n$  sufficiently large.

*Proof.* 1. Theorem 2 shows that  $\tau_{\text{top}}$ , the first time that the original bottom card has come to the top and been inserted into the deck is a strong uniform time for the TTRS.

2. The goal is to show that  $\tau_{\text{top}}$  has the same distribution as  $V$  in Lemma 4. Then the upper bound follows from Lemma 4 and Lemma 3.
3. Write

$$\tau_{\text{top}} = \tau_1 + (\tau_2 - \tau_1) + \cdots + (\tau_{n-1} - \tau_{n-2}) + (\tau_{\text{top}} - \tau_{n-1})$$

where  $\tau_i$  is the time until card  $i$  is placed under the original bottom card.

4. When exactly  $i$  cards are under the original bottom card  $b$ , the chance that the current top card is inserted below  $b$  is  $\frac{i+1}{n}$  and hence the random variable  $(\tau_{i+1} - \tau_i)$  has geometric distribution

$$\mathbb{P}[(\tau_{i+1} - \tau_i) = j] = \frac{i+1}{n} \left(1 - \frac{i+1}{n}\right)^{j-1}$$

for  $j \geq 1$ .

5. The random variable  $V$  in Lemma 4 can be written as

$$V = (V - V_{n-1}) + (V_{n-1} - V_{n-2}) + \cdots + (V_2 - V_1) + V_1$$

where  $V_i$  is the number of draws required until  $i$  distinct balls have been drawn at least once.

6. After  $i$  distinct balls have been drawn, the chance that a draw produces a not-previously-drawn ball is  $\frac{n-i}{n}$ . So  $V_i - V_{i-1}$  has distribution

$$\mathbb{P}[V_i - V_{i-1} = j] = \frac{n-i}{n} \left(1 - \frac{n-i}{n}\right)^{j-1}$$

for  $j \geq 1$ .

7. Comparing, the corresponding terms  $(\tau_{i+1} - \tau_i)$  and  $V_{n-i} - V_{(n-i)-1}$  have the same distribution, since the summands in each sum are independent, it follows that the sums  $\tau$  and  $V$  have the same distribution, as required.
8. To prove the lower bound, fix  $j$  and  $A_j$  be the set of configurations of the deck such that the bottom  $j$  original cards stay in their original relative order. Plainly  $U(A_j) = \frac{1}{j!}$ .

9. Let  $k = k(n) = n \log n - c_n n$  where  $c_n \rightarrow \infty$ . The goal is to show  $P^{k(n)}(A_j) \rightarrow 1$  as  $n \rightarrow \infty$  for fixed  $j$ . Then  $d(k(n)) = \sup\{P^k(A_j) - U(A_j)\} \rightarrow 1$  as  $n \rightarrow \infty$  for fixed  $j$ , establishing the lower bound.
10. To prove  $P^{k(n)}(A_j) \rightarrow 1$  as  $n \rightarrow \infty$ , note  $P^{k(n)}(A_j) \geq \mathbb{P}[\tau - \tau_{j-1} > k]$  because  $\tau - \tau_{j-1}$  is distributed as the time for the card initially  $j$ th from the bottom to come to the top and be inserted. If this has not happened by time  $k(n)$ , then the original bottom  $j$  cards must still be in their relative order at time  $k$ .
11. It suffices to show that  $\mathbb{P}[\tau - \tau_{j-1} \leq k] \rightarrow 0$  as  $n \rightarrow \infty$  for fixed  $j$ . This follows from Chebyshev's inequality. Note that

$$\begin{aligned}\mathbb{E}[(\tau_{i+1} - \tau_i)] &= \frac{n}{i+1} \\ \text{Var}[(\tau_{i+1} - \tau_i)] &= \left(\frac{n}{i+1}\right)^2 \left(1 - \frac{i+1}{n}\right)\end{aligned}$$

and so

$$\mathbb{E}[(\tau - \tau_j)] = \sum_{i=j}^{n-1} \frac{n}{i+1} = n \log n + O(n)$$

and

$$\text{Var}[(\tau - \tau_j)] = \sum_{i=j}^{n-1} \left(\frac{n}{i+1}\right)^2 \left(1 - \frac{i+1}{n}\right) = O(n^2).$$

Then using Chebyshev's inequality gives  $\mathbb{P}[\tau - \tau_{j-1} \leq k] \rightarrow 0$  as  $n \rightarrow \infty$  for fixed  $j$ . □

*Remark.* The strong stationary time property of  $\tau$  played no role in establishing the lower bound. The proof gets lower bounds by guessing some set  $A$  for which  $P^k(A) - U(A)$  should be large and then using

$$d(k) = \|P^k - U\|_{\text{TV}} \geq |P^k(A) - U(A)|.$$

Note that  $n \log n + n \log \epsilon^{-1} = n \log n(1 + o(1))$  and  $n \log n - n \log \epsilon^{-1} = n \log n(1 - o(1))$ . This gives the sense that  $n \log n$  shuffles is about the right number of shuffles needed to bring the deck close to being uniformly shuffled. This gives a cut-off phenomenon, that is  $n \log n$  is a critical number of shuffles

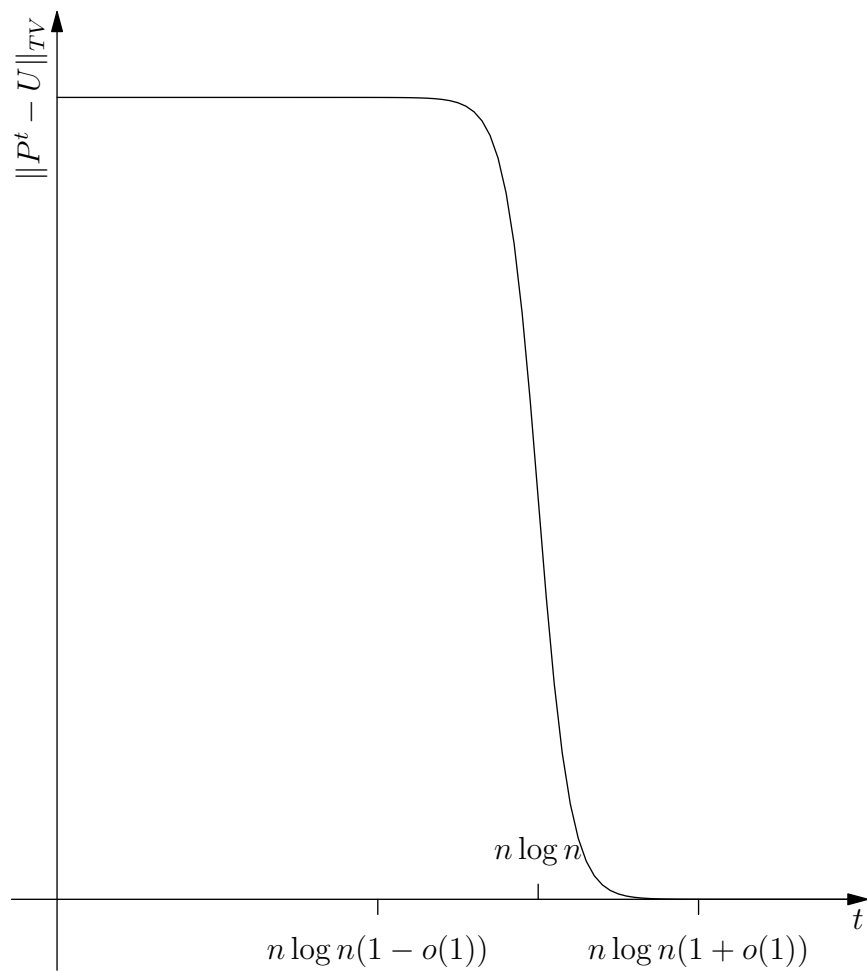


Figure 3: Schematic graph of the cut-off phenomenon for the Total Variation distance of the Markov chain distribution from the uniform distribution as a function of the number of steps.

such that  $d_P(n \log n + o(n)) \approx 0$  but  $d_P(n \log n - o(n)) \approx 1$ . The distance from the stationary density changes abruptly at some value, see Figure 3.

Note that this is quite different from the asymptotics of  $d_P(n) = \|P^n - U\|_{TV}$ . Perron-Frobenius theory says  $d_P(n) \sim a\lambda^n$  where  $\lambda$  is the second largest eigenvalue, but the long-time asymptotics miss the cut-off.

## The Riffle Shuffle

A more realistic model of shuffling a deck cards is the commonly used **riffle shuffle**. The riffle shuffle is sometimes called the GSR shuffle since Gilbert and Shannon and independently Reeds first analyzed it. First cut the deck randomly into two packets, one containing  $k$  cards and the other containing  $n - k$  cards. Choose the number of cards cut,  $k$ , according to the binomial density, meaning that the probability of the cut occurring after  $k$  cards is exactly  $\frac{1}{2^n} \binom{n}{k}$ .

Once the deck is cut into two packets, interleave the cards from each packet in any possible way, such that the cards from each packet keep their own relative order. This means the cards originally in positions  $1, 2, 3, \dots, k$  must still be in the same order after shuffling, even if there are other cards in between. The same goes for cards originally in positions  $k + 1, k + 2, \dots, n$ . This requirement is quite natural, considering how a person shuffles two packets of cards, one in each hand. The cards in the left hand must still be in the same relative order in the shuffled deck, no matter how they interleave with the cards in the other packet, because the cards drop in order while shuffling. The same goes for the cards in the right hand. See Figure 4 for an illustration of a riffle shuffle on a 10-card deck.

A special case of this is the **perfect shuffle**, also known as the **faro shuffle** wherein the two packets are completely interleaved, one card from each hand following one card from the other hand. A perfect shuffle is easy to describe but difficult to perform, except for practiced magicians.

Choose among all possible interleavings uniformly with  $k$  locations among  $n$  places for the first packet, fixing the locations for the cards of the other packet. This is the well-known “stars and bars” counting argument, with the first packet playing the role of the “stars”, the second packet the “bars” creating  $\binom{n}{k}$  possible interleavings. With uniform choice, this means the probability of any one interleaving has probability  $1/\binom{n}{k}$  of occurring. Hence the probability of any particular cut, followed by any particular interleaving is  $\frac{1}{2^n} \binom{n}{k} \cdot 1/\binom{n}{k} = \frac{1}{2^n}$ . Note that this probability has no information about

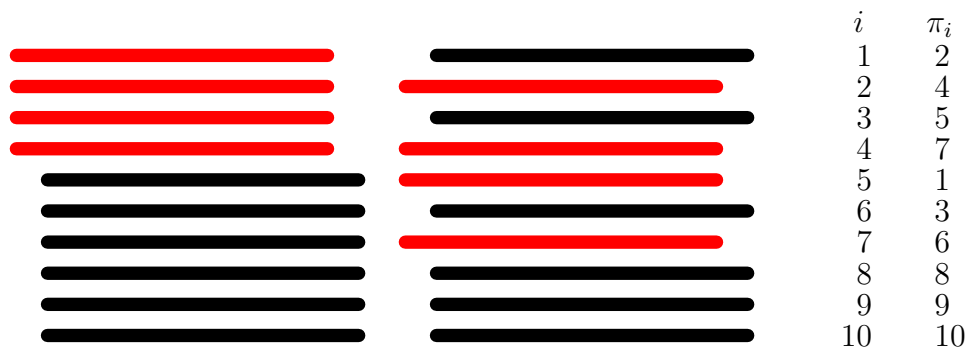


Figure 4: A riffle shuffle on a 10-card deck cut into a top packet of 4 cards and bottom packet of 6 cards.

the cut or the interleaving. The density on possible cuts and interleaving is uniform,.

The uniform density on the set of cuts and interleavings now induces in a natural way a density on the set of permutations. Call the density a *riffle shuffle* and denote it by  $R$ . That is,  $R(\pi)$  is the sum of probabilities of each cut and interleaving that gives the rearrangement of the deck corresponding to  $\pi$ . In short, the chance of any arrangement of cards occurring under riffle shuffling is the proportion of cuts and interleavings that give that arrangement.

*Example.* Consider the riffle shuffle on a 3-card deck as a Markov chain. The probability distribution for  $R$  is in Table 1. To obtain the entries in the transition probability matrix, systematically go through the possible cuts and interleavings. Cutting three cards into the left packet, and none in the right packet, the only possible interleaving trivially leaves the deck unchanged. With a cut into 2 cards on the left, 1 card on the right, one interleaving drops the right packet card on the bottom, the left packet cards as the top 2, leaving the deck unchanged. Two other interleavings move the card in the right packet to the middle or the top. The other two cuts are symmetric to the cuts described above, so 4 of the 8 cuts and interleavings keep the deck in the original order. However, one shuffle each moves the formerly bottom card labeled 3 to the middle or top position, leaving cards 1 and 2 in that order in the shuffled deck. A single riffle shuffle cannot reverse the order of the deck.

To obtain the entries in Table 1 do the computation for a typical element

Table 1: Probability distribution for a riffle shuffle on a 3 card deck.

$\pi$	[123]	[213]	[231]	[132]	[312]	[321]
$Q(\pi)$	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	0.

of the transition probability matrix, say  $p_{\pi,\sigma}$  with  $\pi = [213]$  and  $\sigma = [132]$ . Then  $\pi^{-1} = [213]$  and  $\pi^{-1} \circ \sigma = [231]$ . Now  $R([231]) = \frac{1}{8}$ , giving  $p_{[213][132]} = \frac{1}{8}$  in the probability transition matrix.

The full probability transition matrix under this ordering of the permutations is

$$\begin{array}{c}
 [123] \\
 [213] \\
 [231] \\
 [132] \\
 [312] \\
 [321]
 \end{array}
 \begin{pmatrix}
 [123] & [213] & [231] & [132] & [312] & [321] \\
 \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 \\
 \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{8} \\
 \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & 0 & \frac{1}{8} & \frac{1}{8} \\
 \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} \\
 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & \frac{1}{2}
 \end{pmatrix}.$$

Although in this case, the  $n = 3$  riffle shuffle, the matrix is symmetric, this is in general not true, the riffle shuffle with deck sizes greater than 3 is nonsymmetric, see the exercises.

First note that the Markov chain for riffle shuffling is regular, that is, any permutation has a positive probability of appearing after sufficiently many shuffles, see the exercises. In fact, any number of shuffles greater than  $\log_2 n$  will do. Since the riffle shuffle Markov chain is regular, there is a unique stationary density, which is the uniform density on  $S_n$ .

Starting with the identity ordering, the density of the permutations after 7 riffle shuffles is the first row of  $P^7$ . With matrix multiplication, the density is nearly uniform. In fact,

$$P^7 = \begin{pmatrix}
 0.17059 & 0.16666 & 0.16666 & 0.16666 & 0.16666 & 0.16278 \\
 0.16666 & 0.17059 & 0.16666 & 0.16666 & 0.16278 & 0.16666 \\
 0.16666 & 0.16666 & 0.17059 & 0.16278 & 0.16666 & 0.16666 \\
 0.16666 & 0.16666 & 0.16278 & 0.17059 & 0.16666 & 0.16666 \\
 0.16666 & 0.16278 & 0.16666 & 0.16666 & 0.17059 & 0.16666 \\
 0.16278 & 0.16666 & 0.16666 & 0.16666 & 0.16666 & 0.17059
 \end{pmatrix}.$$

That is, 7 shuffles of the 3-card deck gets close to the stationary density, which turns out to be the uniform density.



## Probability of a Permutation Under Riffle Shuffle

Define a **rising sequence** of a permutation as a maximal increasing subsequence within the permutation, potentially with gaps in position. In more detail applied to shuffled decks of cards, say  $x$  is a particular card from the deck. After the position of  $x$  look for the card labeled  $x + 1$ . If found, repeat the procedure and looking after the  $x + 1$  card for the  $x + 2$  card. Keep going in this manner until it is not possible to find the next card adjacent. Now go back to the original card  $x$  and look for the  $x - 1$  card immediately prior and so on. When done, the subsequence of the permutation containing  $x$  is a rising sequence. A little thought shows that a deck breaks down as a disjoint union of its rising sequences, since the union of any two consecutively increasing subsequences with that element is a rising subsequence.

*Example.* Suppose that a permutation of a deck is 45162378. Start with any card, say 3. Look for 4 and do not find it. Look before the 3 and find 2 and before it, with a gap, find 1. So one of the rising sequences of this permutation is 123. Now start again, this time with say 6. After a gap, find 7 and then after it 8. Before 6 with a gap find 5 and then 4. So another rising sequence is 45678. This accounts for all cards and the deck has only two rising sequences. Writing the sequence as  $45_16_{23}78$ , offsetting the two subsequences, makes this clear.

*Example.* The riffle shuffle in Figure 4 has two rising sequences,  $\pi(1) < \pi(2) < \pi(3) < \pi(4)$  and  $\pi(5) < \pi(6) < \pi(7) < \pi(8) < \pi(9) < \pi(10)$ .

*Example.* Note that  $45_16_{23}78$  is a possible result of a riffle shuffle. Here the cut must divide the deck into two packets such that the length of each is the same as the length of the corresponding rising sequence. So if the deck started in the natural order and the deck is cut into 123 on left and 45678 on the right, then the shuffle interleaves by dropping on the bottom 8, then 7, then 3, then 2, then 6, then 1, then 5 and 4, thus obtaining the given top down order through riffing.

In general, a permutation  $\pi$  of  $n$  cards in original order made by a riffle shuffle will have exactly 2 rising sequences (unless it is the identity with exactly 1 rising sequence). This is a consequence of the definition of a riffle shuffle as a cut and an interleaving. Conversely any permutation of  $n$  cards with 1 or 2 rising sequences can be obtained by a physical shuffle. The lengths of the rising sequences define the size of the cuts, the gaps in a subsequence define the interleavings. Therefore a mathematical definition of a riffle shuffle

can be made as “a permutation with 1 or 2 rising sequences.” Suppose  $c$  cards are cut off the top. Then there are  $\binom{n}{c}$  possible riffle shuffles, (one of which is the identity shuffle). As in Figure 4, after the shuffle, the red and black cards form a binary  $n$ -tuple with  $c$  red cards, there are  $\binom{n}{c}$  such  $n$ -tuples, one of which is the original order. The total number of possible riffle shuffles is

$$1 + \sum_{c=0}^n \left( \binom{n}{c} - 1 \right) = 2^n - n.$$

The next goal is to get similar results about what happens after multiple riffle shuffles. This can be done by considering  $a$ -shuffles. A  **$a$ -shuffle** is another probability density on  $S_n$ . Let  $a$  be any positive integer. Cut the deck into  $a$  packets of nonnegative sizes  $m_1, m_2, \dots, m_a$  with  $m_1 + \dots + m_a = n$  but some of the  $m_i$  may be zero. The probability of this particular packet structure is given by the multinomial density:

$$\frac{1}{a^n} \binom{n}{m_1, m_2, \dots, m_a}.$$

Interleave the cards from each packet in any way, so long as the cards from each packet keep the relative order among themselves. With a fixed packet structure, consider all interleavings equally likely. Count the number of such interleavings as the number of ways of choosing among  $n$  positions in the deck,  $m_1$  places for things of the first type,  $m_2$  places for things of the second type and so on. The count is the multinomial coefficient

$$\binom{n}{m_1, m_2, \dots, m_a}.$$

Hence the probability of a particular rearrangement, i.e. a cut of the deck and an interleaving is

$$\frac{1}{a^n} \binom{n}{m_1, m_2, \dots, m_a} \bigg/ \binom{n}{m_1, m_2, \dots, m_a} = \frac{1}{a^n}.$$

So it turns out that each combination of a particular cut into packets and an interleaving is equally likely, just as in the riffle shuffle. The induced density on the permutations leading to the cuts and shuffles is then called the  $a$ -shuffle, with notation  $R_a$ . The riffle shuffle is just the 2-shuffle, so  $R_2 = R$ .

An equivalent description of the  $a$ -shuffle begins the same way, by cutting the deck into packets multinomially. Then drop cards from the bottom of the packets, one at a time, such that the probability of choosing a particular packet to drop is proportional to the relative size of that packet compared to the number of all cards in the packets. The proof of this description is exactly analogous to the  $a = 2$  case.

A third equivalent description is cutting the deck multinomially into packets of size  $m_1, m_2, \dots, m_n$  and riffing  $m_1$  and  $m_2$  together, meaning choose uniformly among all interleavings that keep the relative order of each packet, then riffing the resulting pile with  $m_3$ , then riffing that resulting pile with  $m_4$  and so on.

It turns out that when performing a single  $a$ -shuffle, the probability of achieving a particular permutation  $\pi$  does not depend on the information contained in  $\pi$ , but only on the number of rising sequences that  $\pi$  has. In other words, the permutations [12534], [34512], [51234], and [23451] have the same probability under any  $a$ -shuffle, since each has exactly two rising sequences.

A useful code through  $n$ -digit base- $a$  numbers specifies how to make a particular  $a$ -shuffle. Here a “shuffle” indicates a particular way of rearranging the deck, not the probability density on all such rearrangements. Let  $A$  be an  $n$ -digit base- $a$  number. Count the number of 0s in  $A$ , this will be the size of the first packet  $m_1$  in the  $a$ -shuffle. Then  $m_2$  is the number of 1s in  $A$  and so on up to  $m_a$ , the number of  $(a - 1)$ s. This cuts the deck into  $a$  packets. Now take the beginning packet of cards of size  $m_1$ . Envision placing these cards on top of all the 0 digits keeping their order as a rising sequence. Do the same for the next packet of size  $m_2$ , placing them on the 1s. Continue up through the  $(a - 1)$ s. This particular way of rearranging the cards will then be the particular cut and the interleaving corresponding to  $A$ . Note that the number of such encodings is  $a^n$ .

*Example.* Let an 8-card deck start in natural order. Let  $A = 23004103$  be the code for a particular 5-shuffle of the 8-card deck. The code has three 0s, one 1, one 2, two 3s and one 4. Thus  $m_1 = 3$ ,  $m_2 = 1$ ,  $m_3 = 1$ ,  $m_4 = 2$  and  $m_5 = 1$ . So cut the deck into 123|4|5|67|8. We put 123 where the 0s are in  $A$ , 4 where the 1 is, 5 where the 2 is, 67 where the 3s are, and 8 where the 4 is. Then get a shuffled deck of 56128437 after applying  $A$  to the natural order.

This code gives a bijective correspondence between  $n$ -digit base- $a$  num-

bers and the set of all ways of cutting and interleaving an  $n$ -card deck according to the  $a$ -shuffle. In fact, if we put the uniform density on the set of  $n$ -digit base- $a$  numbers, this transfers to the correct uniform probability density for cutting and interleaving in an  $a$ -shuffle which means the correct density induced on  $S_n$ .

**Theorem 6.** *The probability of achieving a permutation  $\pi$  when doing an  $a$ -shuffle on an  $n$ -card deck is*

$$\frac{1}{a^n} \binom{n+a-r}{n},$$

where  $r$  is the number of rising sequences in  $\pi$ .

- Proof.*
1. Establish and fix where the  $(a-1)$  cuts occur in an  $a$ -shuffle, then whatever permutations can actually be achieved by interleaving the cards from this cut and packet structure can be achieved in exactly one way: Just drop the cards in exactly the order of the permutation.
  2. Thus the probability of achieving a particular permutation is the number of possible ways of making cuts that could actually cause that permutation, divided by the total number of ways of making cuts and interleaving for an  $a$ -shuffle.
  3. Having  $r$  rising sequences in  $\pi$  determines exactly where  $(r-1)$  of the cuts must have been: between pairs of consecutive cards in the naturally ordered deck such that the first card of the pair ends one rising sequence of  $\pi$ .
  4. This means that we have  $(a-1) - (r-1) = a-r$  unspecified or free cuts that can go anywhere.
  5. So count the number of ways of putting  $a-r$  cuts among  $n$  cards. The standard “stars and bars” combinatorial argument counts

$$\binom{n+a-r}{n}$$

ways to do this, i.e. choosing  $n$  places among  $n + (a-r)$ . This is the numerator of the probability.

6. The denominator is the number of possible ways to cut and interleave for an  $a$ -shuffle. The encoding of the shuffles as the number of  $n$ -digit base  $a$  numbers gives  $a^n$  ways to do this.

□

*Remark.* Compare the results of this theorem with the entries of the matrix

$$\begin{matrix} & [123] & [213] & [231] & [132] & [312] & [321] \\ \begin{matrix} [123] \\ [213] \\ [231] \\ [132] \\ [312] \\ [321] \end{matrix} & \begin{pmatrix} \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 \\ \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & 0 & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} \\ 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} \end{pmatrix} \end{matrix}.$$

Application of the theorem is easier than counting the shuffles carrying one permutation to another.

## Rate of convergence to the stationary distribution

Recall the modeling of card shuffling as a Markov chain. The initial state  $X_0$  is the identity permutation, that is cards in the initial deck order numbered 1 to  $n$ , with probability 1. A particular riffle shuffle, one of a whole family of riffle shuffles, is chosen with a probability distribution from the family. This probability distribution then induces a transition probability from state to state. Going from card order  $\pi$  to  $\sigma$  is the same as composing  $\pi$  with the permutation  $\pi^{-1} \circ \sigma$ . Now identify shuffles as functions on  $\{1, \dots, n\}$  to  $\{1, \dots, n\}$ , that is, permutations. Since a particular riffle shuffle is one of a whole family of riffle shuffles, chosen with a probability distribution  $Q$  from the family, the transition probabilities are  $p_{\pi\sigma} = \mathbb{P}[X_t = \sigma \mid X_{t-1} = \pi] = Q(\pi^{-1} \circ \sigma)$ .

The rate of convergence of  $X_t$  to the stationary density, measured by the total variation distance of some other metric, is determined by the eigenvalues of the transition matrix. We know that the entries of  $P^k$  are the probabilities of certain permutations being achieved under  $k$  riffle shuffles. These probabilities are of the form

$$\frac{1}{2^{nk}} \binom{2^k + n - r}{n},$$

for the probability of a permutation with  $r$  rising sequences being achieved after  $k$  riffle shuffles.

Mann [2] asserts that the eigenvalues of the transition probability matrix for a single riffle shuffle are exactly  $1, \frac{1}{2}, \frac{1}{4}, \dots, \frac{1}{2^n}$ , see the exercises. The second largest eigenvalue determines the rate of convergence to the stationary distribution. For riffle shuffling, this eigenvalue is  $\frac{1}{2}$ . Once the variation distance gets to the cutoff, it decreases by a factor of approximately  $\frac{1}{2}$  with each shuffle.

*Example.* The riffle shuffle matrix for the deck of three cards is

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & 0 \\ \frac{1}{8} & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & 0 & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} & 0 & \frac{1}{2} & \frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} & \frac{1}{8} \\ 0 & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{2} \end{pmatrix}.$$

The eigenvalues of this matrix are  $1, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{4}, \frac{1}{4}$ .

[Section Starter Question]../../../CommonInformation/Lessons/question<sub>mark</sub>.png

## Section Ending Answer

For card players, shuffling the deck to remove any order is essential so that cards dealt from the deck come “at random”, that is, in an order uniformly distributed over all possible deck orders. For the Top-to-Random-Shuffle 7 shuffles of the 3-card deck gets close to the uniform density, which turns out to be the stationary density. With a riffle shuffle on a standard deck, 7 shuffles gets close to the uniform density.

## Sources

This section is adapted from [2]. Parts are also adapted from [1].

---

[Algorithms, Scripts, Simulations]../../../CommonInformation/Lessons/computer.png

# Algorithms, Scripts, Simulations

## Algorithm

## Scripts

---

[Problems to Work]../../../CommonInformation/Lessons/solveproblems.png

## Problems to Work for Understanding

- 1: Show that the Markov chain  $X_t$  on  $S_n$  induced by the TTRS is irreducible.
- 2: Show that the Markov chain  $X_t$  on  $S_n$  induced by the riffle shuffle is irreducible.
- 3: Show that for all  $m, n$

$$\left(1 - \frac{1}{n}\right)^m \leq ne^{-m/n}.$$

- 4: Show with a specific pair of permutations on 4 cards that the transition probability matrix is not symmetric.
- 5: Using a specific example with  $n = 5$  and  $r = 2$  explicitly write out

$$\binom{x + n - r}{n} = \sum_{i=0}^n c_{n,r,i} x^i$$

giving the binomial coefficient as an  $n$ th degree polynomial in  $x$  written in increasing powers with coefficients as a function of  $n$  and  $r$ .

- 6: Show that the entries in the transition probability matrix for the single riffle shuffle on a deck of  $n$  cards are either  $\frac{n+1}{2^n}$ ,  $\frac{1}{2^n}$  or 0.

- 7: Show that the eigenvalues of the transition probability matrix for a single riffle shuffle are exactly  $1, \frac{1}{2}, \frac{1}{4}, \dots, \frac{1}{2^n}$ .

---

[Books]../../../CommonInformation/Lessons/books.png

## Reading Suggestion:

## References

- [1] David Aldous and Persi Diaconis. Shuffling cards and stopping times. *The American Mathematical Monthly*, 93(5):333–348, 1986.
- [2] Brad Mann. How many times should you shuffle a deck of cards. *UMAP Journal*, 15(4):303–332, Winter 1994.

---

[Links]../../../CommonInformation/Lessons/chainlink.png

## Outside Readings and Links:

- 1.
- 2.
- 3.
- 4.

## Solutions

1: The TTRS taking the top card to the bottom of the deck, moving all other cards up one position is an  $n$ -cycle on  $S_n$ . The TTRS taking the top card to the second place in the deck, moving the second card to the top is an *adjacent transposition* of 1 and 2 in that cycle. These two elements are generators of  $S_n$  (see Michael Artin *Algebra*, 1991, Exercise 6.6.16) meaning that any permutation can be achieved by a combination of these actions.

More concretely,  $k$  applications of the TTRS taking the top card to the bottom of the deck will move  $k$  to the top,  $k + 1$ , next and so on to  $n$ , then 1 to  $k - 1$  in the bottom portion of the deck. Then The TTRS taking the top card to the second place in the deck, moving the second card to the top will exchange  $k + 1$  and  $k$ . Then  $n - k$  more applications of the TTRS taking the top card to the bottom of the deck will move the portion 1 to



$k - 1$  back to the top, leaving  $k + 1$  and  $k$  transposed and then  $k + 2$  to  $n$  on the bottom. Thus any adjacent transposition or 2-cycle can be achieved. It is a well known fact that any permutation can be written as a product of 2-cycles, these shuffles are enough to reach any permutation, meaning that the Markov chain is irreducible.

2: By splitting the deck into one card on the left, and  $n - 1$  cards on the right, the specific shuffle taking the top card to the bottom of the deck, moving all other cards up one position is possible. By splitting the deck into one card on the left, and  $n - 1$  cards on the right, the specific shuffle taking the top card to the second place in the deck, moving the second card to the top is also possible. Then by the previous exercises all permutations are possible and the Markov chain is irreducible.

3: The inequality is equivalent to showing

$$m \log\left(1 - \frac{1}{n}\right) \leq \frac{-m}{n}.$$

Since the logarithm function is concave down at  $x = 1$ , then  $\log(1 - \frac{1}{n}) \geq \frac{-1}{n}$ . and the desired inequality follows immediately.

4: Starting with the deck in the order  $[1234]$ , a *perfect in-shuffle* results in the order  $[3142]$ , and this is the only riffle shuffle that results in this order, so  $P_{[1234],[3142]} = \frac{1}{16}$ . On the other hand, no riffle shuffle takes  $[3142]$  to  $[1234]$  because

- splitting the deck into 1 card on the left and 3 cards on the right all interleavings leave 4 above 2,
- splitting the deck into 2 cards on the left and 2 cards on the right all interleavings leave 3 above 1, and
- splitting the deck into 3 cards on the left and 1 card on the right, all interleavings leave 3 above 1.

Therefore,  $P_{[3142],[1234]} = 0$  and the transition probability matrix is not symmetric.

Alternatively, setting  $\pi = [3142]$  and  $\sigma = [1234]$ , then  $P_{[3142],[1234]} = R(\pi^{-1} \circ \sigma)$  where  $R$  is the probability distribution on riffle shuffles. Note that  $\pi^{-1} = [2413]$  and  $\sigma = [1234] = \text{id}$  so  $\pi \circ \sigma = \pi^{-1} = [2413]$ . Note that  $[2413]$  has  $n = 4$  rising sequences. Then by the probability of achieving a

permutation  $\pi^{-1}$  when doing an 2-shuffle on an 4-card deck is

$$\frac{1}{2^4} \binom{4+2-4}{4} = 0.$$

5: The point is to expand

$$\begin{aligned} \binom{x+5-2}{5} &= \binom{x+3}{5} = \frac{(x+3)(x+2)(x+1)x(x-1)}{5!} \\ &= \frac{x^5 + 5x^4 + 5x^3 - 5x^2 - 6x}{5!} \\ &= -\frac{1}{20}x - \frac{1}{24}x^2 - \frac{1}{24}x^2 + \frac{1}{24}x^4 + \frac{1}{120}x^5 \end{aligned}$$

6: The transition probabilities are of the form

$$\frac{1}{2^n} \binom{2+n-r}{n},$$

for the probability of a permutation with  $r$  rising sequences being achieved after a single riffle shuffles. Recall that a permutation  $\pi$  of  $n$  cards in original order made by a riffle shuffle will have exactly 2 rising sequences unless it is the identity which has exactly 1 rising sequence. If  $r = 1$ , then the binomial coefficient will be  $n+1$ , if  $r = 2$  then the binomial coefficient is 1 and if  $r > 2$  the binomial coefficient is 0 by convention.

7: Not a complete solution.

It doesn't really matter what the coefficients are, only that we can write the binomial coefficient expansion as a polynomial in  $x$ . Substituting  $2^k$  for  $x$ , the entries of  $P^k$  have the form

$$\frac{1}{2^{nk}} \sum_{i=0}^n c_{n,r,i} (2^k)^i = \sum_{i=0}^n c_{n,r,n-i} \left(\frac{1}{2^i}\right)^k.$$

This means that the entries of the  $k$ th power of  $P$  are given by fixed linear combinations of the  $k$ th powers of  $1, \frac{1}{2}, \frac{1}{4}$  and  $\frac{1}{2^n}$ . Then from standard facts of linear algebra the set of all eigenvalues of  $P$  (What are these standard facts?) is exactly  $1, \frac{1}{2}, \frac{1}{4}, \dots, \frac{1}{2^n}$ . Further, Mann [?, mann96] asserts that the multiplicities are the Stirling numbers of the first kind, up to sign:

$$\text{multiplicity} \left( \frac{1}{2^n} \right) = (-1)^{n-i} c(n, k)$$

referencing Graham, Knuth, Patashnik, *Concrete Mathematics*, 1989, p. 243-253.

---

I check all the information on each page for correctness and typographical errors. Nevertheless, some errors may occur and I would be grateful if you would alert me to such errors. I make every reasonable effort to present current and accurate information for public use, however I do not guarantee the accuracy or timeliness of information on this website. Your use of the information from this website is strictly voluntary and at your risk.

I have checked the links to external sites for usefulness. Links to external websites are provided as a convenience. I do not endorse, control, monitor, or guarantee the information contained in any external website. I don't guarantee that the links are active at all times. Use the links here with the same caution as you would all information on the Internet. This website reflects the thoughts, interests and opinions of its author. They do not explicitly represent official positions or policies of my employer.

Information on this website is subject to change without notice.

Steve Dunbar's Home Page, <http://www.math.unl.edu/~sdunbar1>

Email to Steve Dunbar, `sdunbar1 at unl dot edu`

Last modified: Processed from L<sup>A</sup>T<sub>E</sub>X source on October 13, 2020